Capítulo 1

Introducción

1.1. Motivación

- La seguridad en dispositivos móviles se ha convertido en un asunto muy importante debido al incremento de ataques recibidos y a las consecuencias que éstos tienen.
- Los ataques están incentivados por la popularización de los dispositivos móviles, el aumento de información personal y confidencial que almacenan y las operaciones realizadas a través de ellos, como por ejemplo las bancarias.
- Actualmente, más del 99 % de los dispositivos móviles en el mercado tiene a iOS o Android como su sistema operativo. El número actual de aplicaciones de Android en el mercado supera los 3.500.00 y para iOS asciende a más de 3.100.000.
- Además, debido al uso diario de estas aplicaciones, se puede filtrar una gran cantidad de información privada y confidencial a menos que se aplique control de acceso a las aplicaciones instaladas.

Motivación I Este trabajo realiza un análisis detallado sobre las características de seguridad en Android e iOS, con el objetivo de preservar la privacidad del usuario.

Motivación II Sumado al análisis, se presenta un *framework* comparativo, cuyas principales funciones son:

- Determinar empíricamente los alcances de los sistemas de permisos.
- Establecer una relación entre los permisos presenten en ambas plataformas.

Capítulo 2

Análisis Comparativo

- Existen muchos trabajos sobre distintas formas de comparar la seguridad de ambas plataformas.
- Cada uno de ellos propone una medida de comparación que focaliza el análisis en alguna característica particular de Android y/o de iOS.
- Esta tesina propone analizar distintas características presentes en ambas plataformas, poniendo foco en los permisos que se pueden modificar *en tiempo de ejecución*.

Se analizaron cuatro características presentes en iOS y Andriod:

- Arranque verificado
- Cifrado del sistema de archivos
- Bloqueo del dispositivo
- Seguridad de las aplicaciones

Se pone foco especialmente en los sistemas de permisos:

Al comparar la gestión de permisos de ambas plataformas, encontramos varias similitudes:

- A una aplicación se le otorga permisos básicos al momento de instalación, sin posibilidad de revocarlos.
- Si una aplicación necesita un permiso no básico, debe requerirlo. El usuario puede otorgarlo o revocarlo.
- Desde la configuración de privacidad, el usuario puede revocar u otorgar permisos a las aplicaciones.

Respecto a cómo se definen los permisos, se observan diferencias de concepto:

- En Android están orientados según el riesgo implícito al otorgarlos.
- En iOS los permisos están orientados a los componentes.

Sin embargo, se pueden comparar según los componentes que son afectados por un permiso, resultando la siguiente Tabla:

Respecto del alcance del sistema de permisos, se observó una falta de granularidad de los permisos que se pueden modificar *en tiempo de ejecución*:

- En Android, un permiso es a nivel de grupo. Por lo tanto, el usuario otorga o deniega para todo el grupo.
- La misma situación ocurre en iOS: se otorga un permiso de acceso a todas las funcionalidades de un determinado componente.

Como consecuencia de ello, el usuario está delegando a una aplicación demasiados permisos y no tiene expresividad para decir qué funcionalidades autoriza.

Otra cosa a destacar es la cobertura del sistema de permisos. Las dos plataformas dejan funcionalidades principales del dispositivo sin permisos modificables *en tiempo de ejecución*:

- En Android se destacan: Acceso a Internet, Compartir vía Bluetooth e Información del Dispositivo.
- En iOS se destacan: Acceso a Internet y SMS. Tampoco tiene la suficiente granularidad para administrar el acceso a los datos de las llamadas telefónicas.

Para finalizar analizamos cómo se muestran al usuario los permisos adquiridos por una aplicación:

Capítulo 3

Hacia un Framework para la Comparación de Permisos

- Android e iOS permiten cambiar ciertos permisos de una aplicación luego de haberla instalado en el dispositivo.
- Es por ello que se ha desarrollado un *framework* para determinar empíricamente el alcance de los sistemas de permisos de ambas plataformas.

Objetivo I Se busca dejar en evidencia posibles vulnerabilidades presentes en los modelos de seguridad.

Objetivo II Se pone énfasis en la relación existente entre la privacidad del usuario y el sistema de permisos, analizando cuál es la cobertura del sistema respecto de los datos sensibles para la privacidad.

Aplicación Híbrida Es una aplicación móvil diseñada en un lenguaje de programación web ya sea HTML5, CSS o JavaScript, junto con un *framework* que permite adaptar la vista web a cualquier vista de un dispositivo móvil.

Apache Cordova Es un *framework* que permite crear aplicaciones para dispositivos móviles utilizado HTML5, CSS3, y JavaScript, con el objetivo de lograr un desarrollo multiplataforma.

El *framework* es una aplicación móvil híbrida desarrollada con Apache Cordova y está compuesto por varios tests.

Cada test pone a prueba a un componente del dispositivo, permitiendo así conocer el alcance de los permisos correspondientes a dicho componente.

- Para el presente trabajo se decidió utilizar los emuladores oficiales para testear el *framework* propuesto.
- Los emuladores permiten interactuar de la misma manera que se haría con un dispositivo real, pero con el ratón y el teclado, y mediante los botones y los controles del emulador.

Para cada uno de los tests se detalla el algoritmo, los plugins de Apache Cordova que se utilizaron para desarrollarlo y una serie de capturas que muestran los casos exitosos y fallidos.

Luego de correr los tests, se puenden clasificar los componentes testeados en cuatro clases mutuamente excluyentes, según requieran autorización del usuario para utilizarlos.

Capítulo 4

Conclusiones y Trabajos Futuros

Primer Aporte Se realizó un análisis comparativo entre algunas características presentes en los modelos de seguridad de ambas plataformas.

Ellas son: verificación del arranque del sistema operativo, cifrado del sistema de archivos, bloqueo del dispositivo y sistemas de permisos.

Todas ellas se eligieron porque son importantes a la hora de resguardar la privacidad del usuario.

Segundo Aporte Como fruto del análisis, se logró establecer una medida de comparación entre los permisos presentes en ambas plataformas. La medida propuesta es la siguiente: *dos permisos son similares si resguardan un componente que provee la misma funcionalidad.*

Utilizando la medida propuesta, todos los permisos que un usuario puede cambiar en tiempo de ejecución quedan clasificados en tres grupos: *Ambas Plataformas*, *Solo en Android* o *Solo en iOS*. Cabe aclarar que los grupos son mutuamente excluyentes.

Tercer Aporte Otro aporte es el *Framework para la Comparación de Permisos*. Tiene dos funciones principales: determinar empíricamente los alcances de los sistemas de permisos; y establecer una relación entre los permisos presenten en las dos plataformas.

El *framework* está compuesto por una batería de tests, teniendo cada uno de ellos la tarea de probar una funcionalidad provista por Android e iOS.

Cuarto Aporte Como resultado de la utilización del *framework* se determinó una clasificación de permisos. El criterio utilizado fue: *un componente pertenece a una clase según requiera autorización explícita del usuario para*

utilizarlo. Para finalizar, se enumeran algunas líneas a seguir como trabajos a futuro:

- Probar y mejorar los test que actualmente conforman el framework en dispositivos reales.
- Desarrollar tests para las funcionalidades que no pueden ser emuladas (ver Seccion 5.1.1).
- Desarrollar un test para poder comparar el cifrado de archivos.
- Android otorga todos los permisos *normales*, tal como se enuncia en la Seccion 3.1.4. Pero no sabemos qué permisos otorga iOS. Se podrían desarrollar varios test para descubrirlos.
- Dado que salieron al mercado las versiones Android 8.0 e iOS 11, se podría analizar extender el *framework* para las características de seguridad adicionadas en dichas versiones.
- En el Capítulo 4 se mencionan algunos análisis previos relacionados a la seguridad de Android y/o de iOS. Se podría profundizar más en comparar el modelo propuesto en el presente informe con los análisis mencionados previamente.